Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001524

International filing date: 02 February 2005 (02.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-025015
Filing date: 02 February 2004 (02.02.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/001524

日本国特許庁
JAPAN PATENT OFFICE

03. 2. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

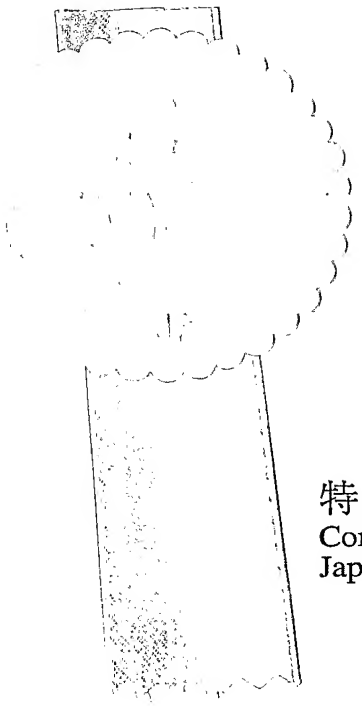
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月　２日

出願番号
Application Number: 特願２００４－０２５０１５

[ST. 10/C]: ［Ｊ Ｐ ２００４－０２５０１５］

出願人
Applicant(s): 株式会社サイバー・ソリューションズ



２００５年　３月　９日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２００７９

【書類名】　特許願
【整理番号】　CYBER001
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　宮城県仙台市青葉区南吉成６－６－３
　【氏名】　キニ　グレン　マンスフィールド
【特許出願人】
　【識別番号】　501175281
　【氏名又は名称】　株式会社サイバー・ソリューションズ
【代理人】
　【識別番号】　100088096
　【弁理士】
　【氏名又は名称】　福森　久夫
　【電話番号】　03-3261-0690
【手数料の表示】
　【予納台帳番号】　007467
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0306732

【書類名】特許請求の範囲
【請求項１】
インターネット回線を通じて送信されてきたパケットの送信件数と送信元アドレス件数とを監視し、そのパケットの送信件数が一定時間内で所定数に達すると共に送信元アドレス件数が略同期して所定数若しくは所定率に達した場合にはその大量のパケットをスパムと判定する判定手段を備えたことを特徴とするスパム検知システム。
【請求項２】
インターネット回線を通じて送信されてきたパケットのパケット数と送信元アドレス件数とを監視し、そのパケットのパケット数が一定時間内で所定数に達すると共に送信元アドレス件数が略同期して所定数若しくは所定率に達した場合にはその大量のパケットをスパムと判定する判定手段を備えたことを特徴とするスパム検知システム。
【請求項３】
インターネット回線を通じて送信されてきたパケットの送信件数と送信元アドレス件数とを監視し、そのパケットの送信件数が一定時間内で所定数に達すると共に送信元アドレス件数が略同期して所定数若しくは所定率に達した場合にはその大量のパケットをスパムと判定する判定手段とを備え、インターネットの複数個所での判定結果を比較することにより送信元を探索するようにしたことを特徴とするスパム元探索システム。

【書類名】明細書
【発明の名称】スパム検知システム及びスパム元探索システム
【技術分野】
【０００１】
本発明は、インターネット回線を通じて送信されてきた電子メールが適正な電子メールかスパムメールかを判定するメール受信システム関するものである。
【背景技術】
【０００２】
【特許文献１】特開２００３－３１８９８７号公報
【特許文献２】特開２００３－２３４７８４号公報　近年、ある企業や組織をターゲットにし、特定メールサーバーの不特定メールアカウントに対し、電子メールを大量に送信するスパムメール（迷惑メール・嫌がらせメール）が問題となっている。このようなスパムメールは、一般には１メールアカウント毎に割り当てられるメールサーバー（メールＢＯＸ）の容量を超えるように多数の電子メールを一度に送りつけることで他の電子メールを受信させないようにしたり、課金制ユーザーに対するプロバイダへのアクセス時間並びに通信会社への通信時間を延長させて納付料金を高騰させるといった弊害を与えるものである。いわゆるＤｏＳ攻撃といわれるものである。ＤｏＳ攻撃とは、攻撃対象機器に処理能力を上回る非常に甚大な数のパケットを送りつけ、対象のサービスを不能にしてしまう攻撃方法である。
【０００３】
そこで、電子メールのデータフォーマットのヘッダ部分に含まれるＦｒｏｍアドレス（送信元アドレス）を管理し、このようなスパムメールを送りつけたメールアドレスからの電子メールを２度と受信しないと共にその送信元に電子メールを送り返すといった防止機能を付加したサービスが見受けられる。
【０００４】
しかしながら、このような防止サービスは、異なったメールアドレスから再びスパムメールを送りつけてきた場合には、そのスパムメールの受信を拒否することができないといった問題が生じていた。
【０００５】
一方、このようなスパムメールを送りつける送信元では、受信拒否されたスパムメールが送り返されてしまうと、自身のメールサーバーが容量オーバーとなってしまう。従って、送信元では、Ｆｒｏｍアドレスをランダムに偽造作成し、大量の電子メールの各メールアドレスを異ならせたうえで特定メールアドレスにスパムメールを送信するといった対応で対抗してきているのが実情である。
【０００６】
これに対し、例えば、特許文献１では、不特定多数の電子メールに対し、電子メールのデータフォーマットのヘッダ部分に含まれるＴｏアドレス（送信先アドレス）を事前設定されたアカウント別メールヘッダ・コンテンツ書き換え定義にしたがい、受信した電子メールを書き換えた上でその書き換えメールアドレスに再送信（転送）し、特定メールサーバーへの負荷を分散させている。
【０００７】
また、特許文献２では、同時に送信されてきた電子メールのＦｒｏｍアドレスに不明なものを大量に含むか否かを判定し、Ｆｒｏｍアドレスに不明なものが大量に含まれている場合には、その送信されてきた大量の電子メールのＦｏｒｍアドレスに送信メールを返信し、返信できた電子メールのみを適正な電子メールとして受信している。
【発明の開示】
【発明が解決しようとする課題】
【０００８】
ところで、上記特許文献１に開示の技術は、電子メールの受信許可・拒否等のチェック機能を利用しているため、電子メールの受信許可の設定若しくは受信拒否を予め設定しな

ければならず、大量のメールアドレスに対応することは非常に困難である。

【０００９】

また、上記特許文献２に開示の技術においても、同時に送信されてきた電子メールのＦｒｏｍアドレスに不明なものを大量に含むか否かを判断したうえで不明なＦｒｏｍアドレスに対して送信されてきた電子メールを送り返していることから、事前に不明と判断するためのＦｒｏｍアドレスの登録を必要としている。

【００１０】

また、送り返すことができなかった電子メールの中に、例えば、ユーザー登録しているプロバイダやソフトウエア販売会社から送信オンリーで設定された重要な案内メール（例えば、サービスメンテナンスのためのサーバー停止案内メール、アクセスポイント変更・設定の案内メール、販売したソフトウエアプログラム中のバグの発見に伴うお知らせメール等）を受信することができなくなる虞れがあった。

【００１１】

このように、従来技術では、スパムメールの判定基準が複雑となっているため、１度目のスパムメールの受信を余儀なくされたり、必要な電子メールをも受信拒否してしまうといった問題が生じていた。

【００１２】

本発明は、上記問題を解決するため、スパムメールであるか否かの判定基準を容易化することができるメール受信システムを提供することを目的とする。

【課題を解決するための手段】

【００１３】

本発明のスパム検知システムは、インターネット回線を通じて送信されてきたパケットの送信件数と送信元アドレス件数とを監視し、そのパケットの送信件数が一定時間内で所定数に達すると共に送信元アドレス件数が略同期して所定数若しくは所定率に達した場合にはその大量のパケットをスパムと判定する判定手段を備えたことを特徴とする。

他のスパム検知システムは、インターネット回線を通じて送信されてきたパケットのパケット数と送信元アドレス件数とを監視し、そのパケットのパケット数が一定時間内で所定数に達すると共に送信元アドレス件数が略同期して所定数若しくは所定率に達した場合にはその大量のパケットをスパムと判定する判定手段を備えたことを特徴とする。

本発明のスパム元探索システムは、インターネット回線を通じて送信されてきたパケットの送信件数と送信元アドレス件数とを監視し、そのパケットの送信件数が一定時間内で所定数に達すると共に送信元アドレス件数が略同期して所定数若しくは所定率に達した場合にはその大量のパケットをスパムと判定する判定手段とを備え、インターネットの複数個所での判定結果を比較することにより送信元を探索するようにしたことを特徴とする。

【発明の効果】

【００１４】

本発明のメール受信システムによれば、同時に大量に送信されてきた電子メールに対し、その大量の電子メールの送信件数又はパケット数が一定時間内に所定数に達した時に、略同期して送信元アドレス件数が所定数若しくは所定率に達した場合には、その大量の電子メールをスパムメールと判定することにより、特定のＦｒｏｍアドレスに対して受信許可設定若しくは受信拒否設定をするといった細かく煩わしい設定をすることなくスパムメールが送信されてきたことを認識することができる。

【発明を実施するための最良の形態】

【００１５】

前述した通り、ＤｏＳ攻撃とは、攻撃対象機器に処理能力を上回る非常に甚大な数のパケットを送りつけ、対象のサービスを不能にしてしまう攻撃方法である。

このＤｏＳ攻撃は次のような特徴を有している。

【００１６】

発信元アドレスは偽造されている　（偽のアドレスが用いられている）攻撃元の発信元アドレスであるパケットをフィルタすることにより、ＤｏＳ攻撃をブロックされないよう

に、ＤｏＳ攻撃の発信元アドレスはランダムに選択されていることが一般的である。

【００１７】

ＤｏＳは非常に莫大なパケットが送信されるので、次にような方法で検知される。

【００１８】

第１の方法は、攻撃パケットもしくは、不正なパケットの数を数える方法である。どのようなパケットが不正であるかを判断することはむずかしい。なぜなら、ＤｏＳ攻撃に使われるパケット一つ一つは正常なパケットであるからである。

【００１９】

第２の方法は、検知したパケット全て（攻撃パケットも含む）を数える方法である。ネットワークトラフィックは時々刻々動的に変化する。従って、単にネットワークトラフィック量が増大したからといって、その現象はＤｏＳ攻撃によるものだと指摘することはできない。また、既にトラフィック量が飽和状態である場合は、ＤｏＳ攻撃があったとしても、トラフィック量は増加しない。

【００２０】

それに対して、本形態における方法は、ＤｏＳ攻撃の検知方法は、トラフィックの発信元アドレスを数える方法である。もし攻撃者がランダムに発信元アドレスを選択しているならば、観測される発信元アドレスの数も増加しているはずである。ある一定時間間隔では、１個の発信元アドレスに対して、そのような発信元アドレスを持つパケットは複数観測されるのが通常である。しかし、攻撃の最中では一般的に１個の（偽造された）発信元アドレスに対して、攻撃パケットは１個しか観測されない。このようにＤｏＳ攻撃を検知することができる。

【００２１】

発信元アドレス、到達先アドレスとその他の情報・データから構成されている。時間間隔でパケットを数える。例えば、図４に示すように、ネットワーク（Ｎｅｔ１）と攻撃先（Ｔａｒｇｅｔ）との間の経路にパケットを観測するための手段を設けておき、そこで、パケットを観測すればよい。かかる手段としては、例えばスニファー（Ｓｎｉｆｆｅｒ）やパッシブ型プローブなどの機器がある。

【００２２】

スニファ（Ｓｎｉｆｆｅｒ）や、パッシブ型プローブなどの機器は全てのパケットを観測でき、それらの機器は以下の値を数えあげることができる

パケットの全数
ある特定の発信元アドレスを持つパケット数
ある特定の到達先アドレスを持つパケット数
発信元アドレス毎のパケット数
到達先アドレス毎のパケット数
特定のタイプのパケット数

これらの値は、一定時間間隔毎に収集可能である。

【００２３】

次にＤｏｓ攻撃の追跡方法について述べる。

【００２４】

ＤｏＳ攻撃元の追跡方法としては、第１に、不正なパケットの経路をチェックする（パケット追跡）方法がある。しかし、どのようなパケットが不正なのかを知る必要がある。

【００２５】

第２に、トラフィックパターンをチェックする方法がある。しかし、この方法は、不正確である。

【００２６】

それに対して、本発明の実施の形態においては、経路上において観測されるアドレス数の変化をチェックする方法である。全ての経由地で同様な現象が観測されると推測される以下のようなパターンが観測される。

【００２７】

時間（任意単位）	パケット数	発信元アドレス数
1	１０００	５０
2	８００	６０
3	９００	５７
4	１２００	６４
5	５０	３０
6	１５００	５３０
7	１８００	５５０
8	１７００	５７０
9	８００	８０
１０	９００	６５

上記において、時間６、７、８においては、パケット数とともに発信元アドレス数が増加している。そこでは、ＤｏＳ攻撃がなされている。
一方、図５に示すように、インターネットの各経路にスニファーＳｎ（ｎ＝１，２，３，・・・）を置いておき、そこでの観測結果同士を比較すればどの経路でＤｏＳ攻撃がなされているかを知ることができる。その経路を遮断すればＤｏＳ攻撃元を追跡することができ、必要に応じてその経路を遮断すればよい。また、その経路からの所定のパケットを遮断すればよい。

【実施例】

【００２８】

次に、本発明のメール受信システムの実施の形態を図面に基づいて説明する。

【００２９】

図１は本発明のメール受信システムを示す図である。図１において、１はインターネット回線、２はインターネット回線１に接続された送信元のコンピュータ本体、３はインターネット回線１に接続された受信側コンピュータ、４はインターネット回線１と受信側コンピュータ３との間に接続されたメール監視装置である。

【００３０】

尚、このメール監視装置４にはルータ等が用いられるが、受信側コンピュータ３がメールサーバー等であった場合には、そのメールサーバーをメール監視装置４としても良い。この場合、受信とはメールサーバーで割り当てたメールアカウント毎のメールＢＯＸへの受信を意味、判定のためのメールサーバー上での受信は含まないものとする。また、受信側コンピュータ３がプロバイダ所有のメールサーバーであった場合には、他のインターネット回線を通じてメール受信端末（例えば、パーソナルコンピュータ等）が接続されることとなる。

【００３１】

通常、送信側コンピュータ２から送信される電子メールは、図２（Ａ）に示すように、その電子メールを構成するパケットのパケットデータフォーマット１０のヘッダ部１１に、送信元メールアドレスに相当するＦｒｏｍアドレス１２と送信先アドレス（受信側アドレス）に相当するＴｏアドレス１３とが含まれている。

【００３２】

メール監視装置４は、送信された電子メールの件数若しくはパケット数と、Ｆｒｏｍアドレス１２の件数とを監視する。

【００３３】

例えば、通常の電子メールの送受信を想定した場合、送信元コンピュータ２から受信側コンピュータ３に送信される電子メールの件数は１件であり、例え、他の送信側コンピュータ（図示せず）から略同時期に電子メールが受信側コンピュータ３に送信されたとしても、その電子メールの件数とＦｒｏｍアドレス１２とは１対１で比例して増える。

【００３４】

また、例えば、近年のメールサーバーでは、コンピュータウイルスを含む電子メールの受信を拒否するため、１つのパケットデータフォーマット１０が所定量以上であった場合

、その受信を拒否するようになっている。

【００３５】

このため、電子メール送信側では、本来であれば１件の電子メールに添付して送信したい複数のデータ（例えば、ＰＤＦファイル等）を複数件の電子メールに分割し、その分割した複数の電子メールを一斉に送信する場合がある。

【００３６】

このような場合、メール監視装置４では、図２（Ｂ）のピークＰ１に示すように、電子メールの件数は通常の電子メールの送信件数よりも多い件数の電子メールが送信されてきた判定する。

【００３７】

しかしながら、各電子メールのＦｏｒｍアドレス１２は共通であることから、その電子メールを正式に受信する。尚、メール送信件数が所定数以内であった場合（例えば、１０件未満）に、その受信を許容するようにしても良い。

【００３８】

一方、実際には１台の送信側コンピュータ２から送信された電子メールでありながら、送信メールアドレス（Ｆｒｏｍアドレス１２）をランダムに偽装して大量の電子メールを受信側コンピュータ３に送信してきた場合、メール監視装置４では、図２（Ｂ）及び図２（Ｃ）のピークＰ２，Ｐ３に示すように、電子メールの数（若しくはパケット数）が通常の電子メール送受信のときよりも多くなると同時に、その各電子メールのＦｏｒｍアドレス１２も略同時期に増大することになる。

【００３９】

従って、電子メールの数（若しくはパケット数）が所定数（例えば、１００件）を越えた際、Ｆｒｏｍアドレス１２の数も略同時期に所定数（例えば、９０件）若しくは所定率（例えば、電子メールの数に対して９０％）を超えた場合には、その受信を拒否する。

【００４０】

尚、このような一斉同時送信に対応した一定時間内に送信されてきた電子メールの件数（若しくはパケット数）の所定数並びにＦｒｏｍアドレス数の所定数の設定は、メールサーバー上で設定されたメール受送信容量（メールＢＯＸの割当容量等）に応じたり、受信側コンピュータ３の所有者の業種等に応じたりして設定することができる。

【００４１】

例えば、受信側コンピュータ３の所有者の業種が旅行代理店やイベント企画会社であった場合、人気のある旅行プランやイベント内容に対する申込メールが殺到するといったことが想定される。

【００４２】

従って、これらの業種等では、日常的に電子メールの受信件数も多いことが想定できるため、その平均的な受信件数を考慮して所定値（件数等）を設定すればよい。

【００４３】

また、このような申込メールが殺到した場合であっても、スパムメールに相当するような全く同じ時間（瞬間的）に大量の申込メールが送信されてくることは稀であると想定されるが、判定のための一定時間の設定を短くするといった設定変更でも対応は可能である。

【図面の簡単な説明】

【００４４】

【図１】本発明のメール受信システムの概念図である。

【図２】（Ａ）は電子メールのパケットデータフォーマットの説明図、（Ｂ）は電子メールの送信件数の一例を時系列で示したグラフ図、（Ｃ）は電子メールのアドレス件数の一例を時系列で示したグラフ図である。

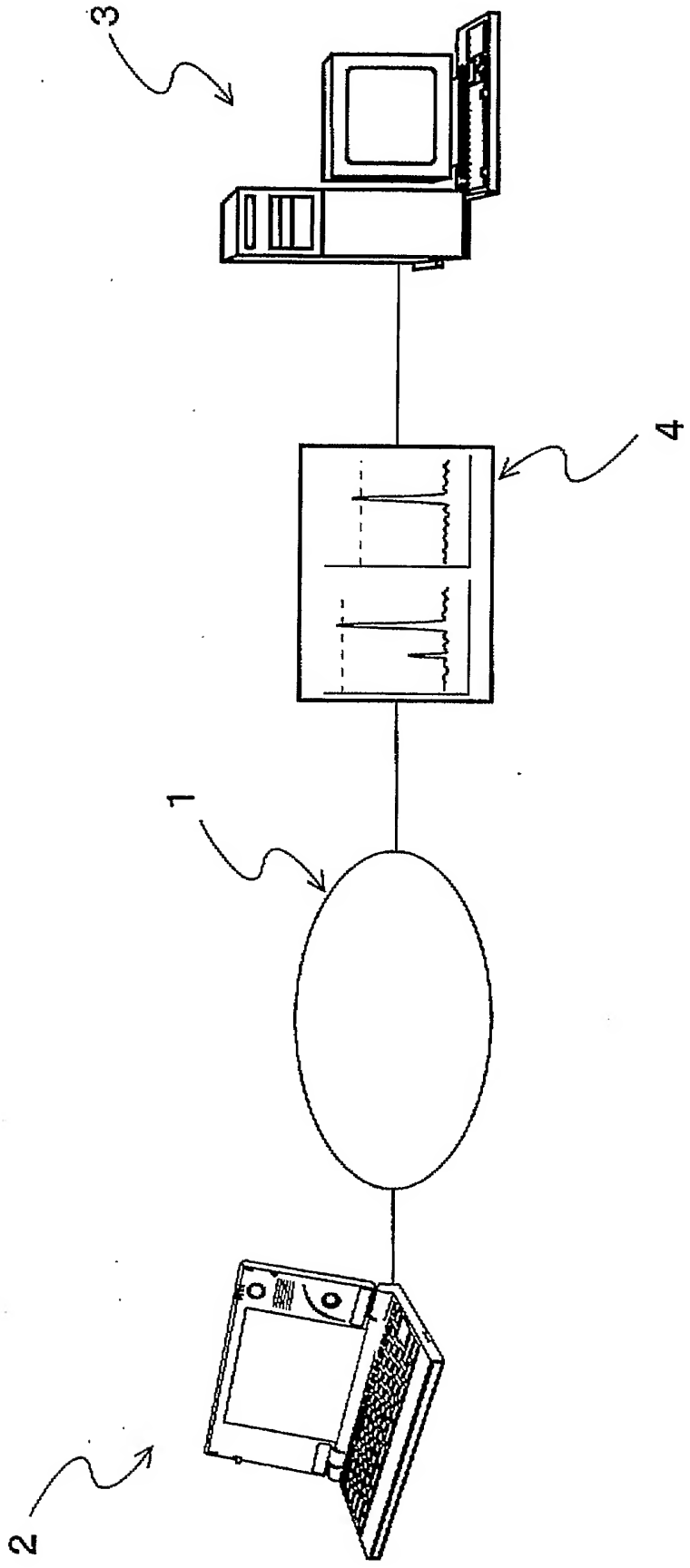
【図３】パケット探索を示す概念図である。

【図４】インターネットのシステムを示す概念図である。

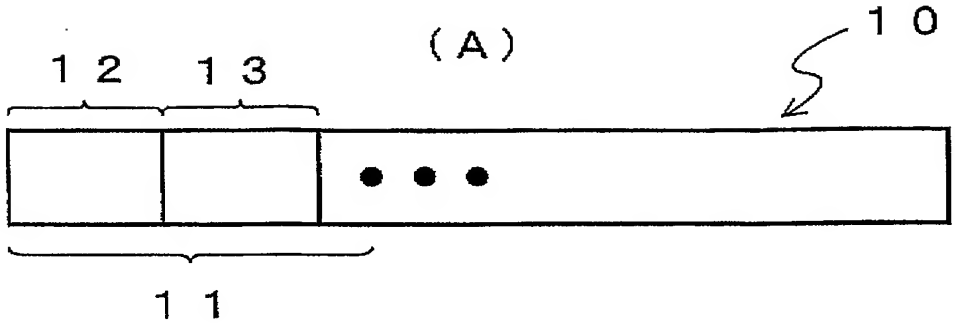
【符号の説明】

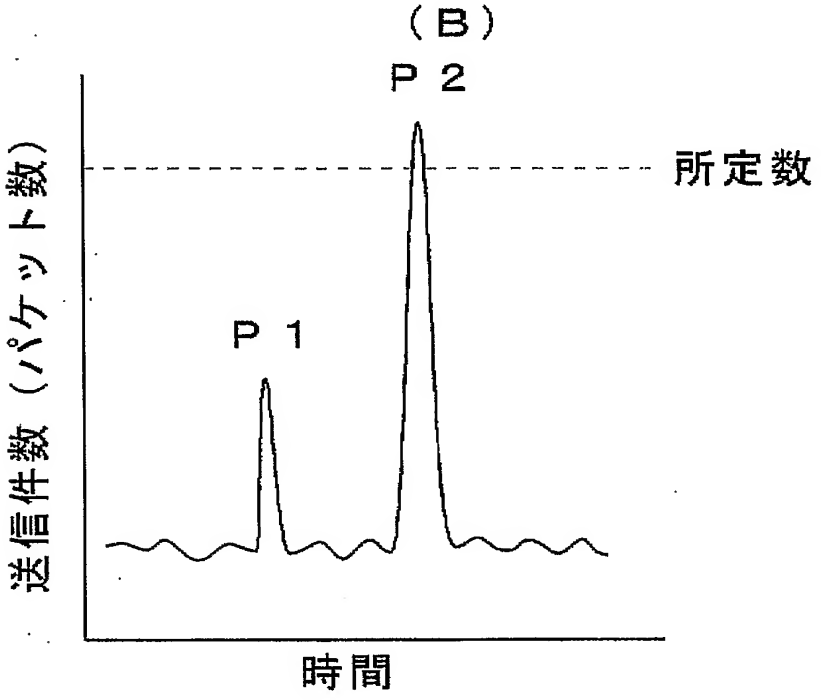
【００４５】
１…インターネット回線
２…送信側コンピュータ
３…受信側コンピュータ
４…メール監視装置（判定手段）

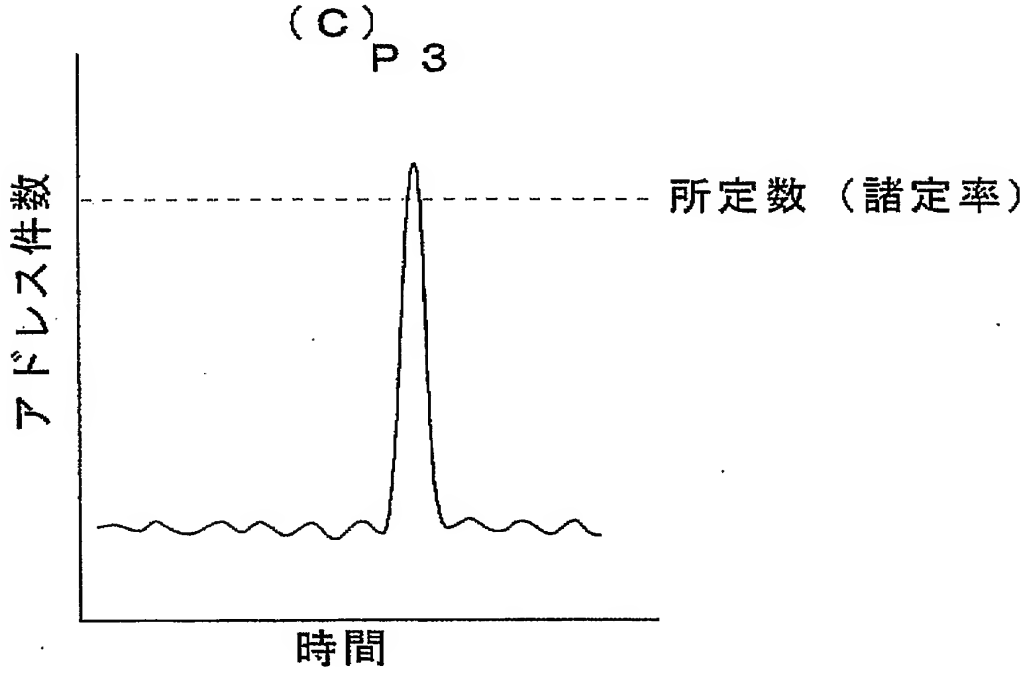
【書類名】図面
【図１】



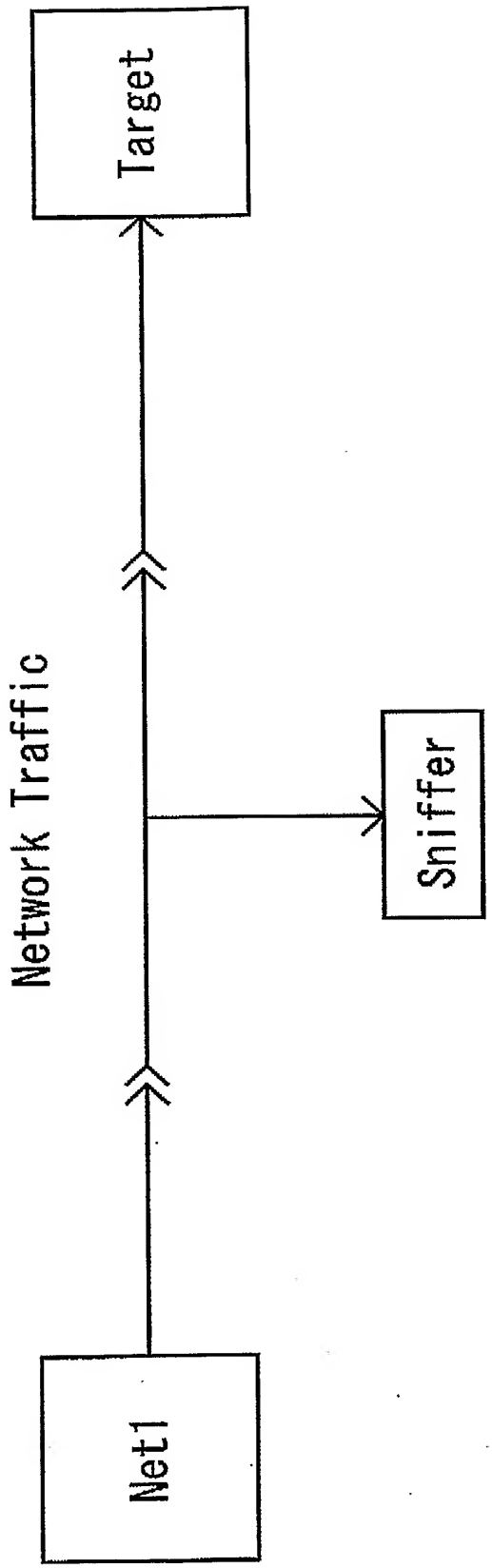
【図２】



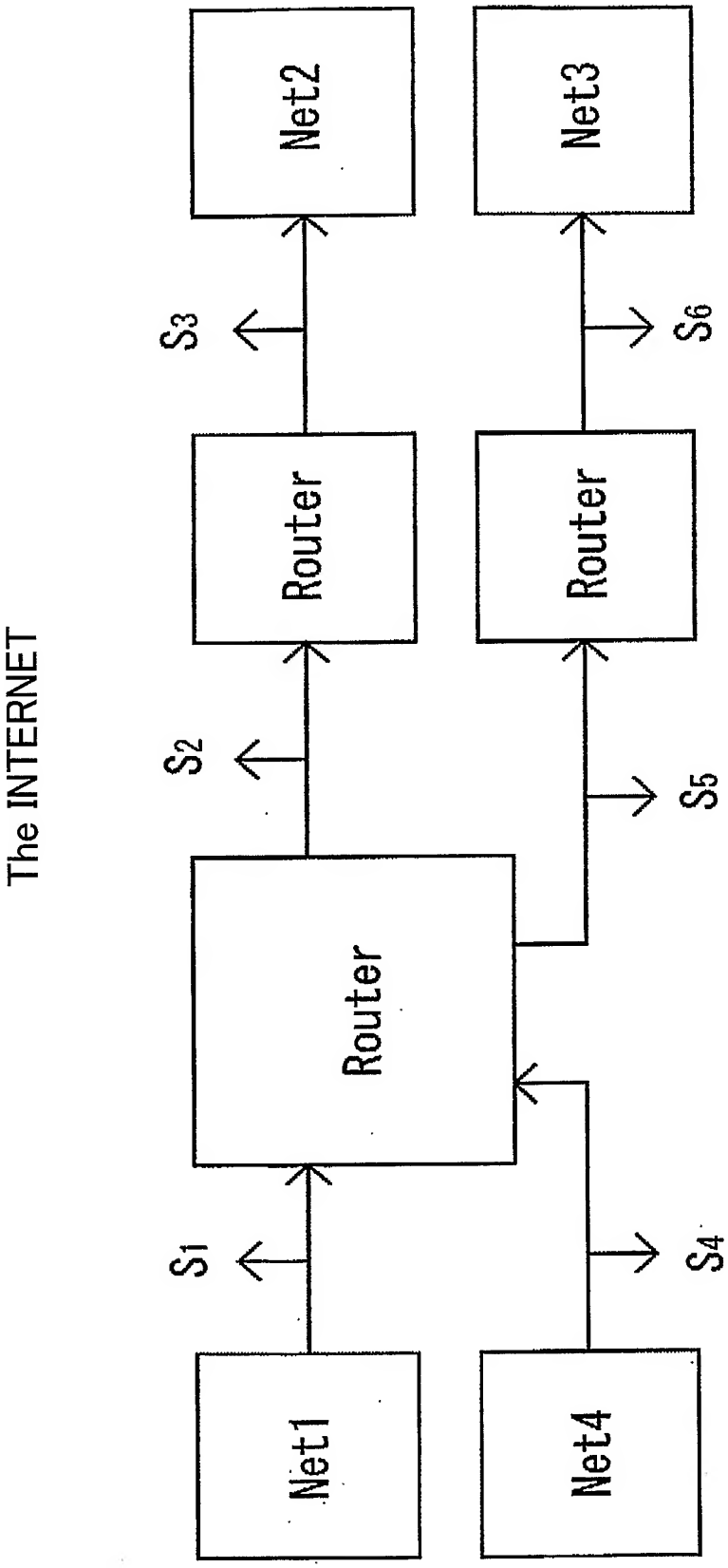




【図３】



【図４】


The INTERNET
Net1
Net2
Net3
Net4
Router
Router
Router
S1
S2
S3
S4
S5
S6

【書類名】要約書
【要約】
【課題】スパムメールであるか否かの判定基準を容易化することができるメール受信システムを提供すること。
【解決手段】同時に大量に送信されてきた電子メールに対し、その大量の電子メールの送信件数又はパケット数が一定時間内に所定数に達した時に、略同期して送信元アドレス件数が所定数若しくは所定率に達した場合には、メール監視装置４がその大量の電子メールをスパムメールと判定する。
【選択図】図１

認定・付加情報

特許出願の番号	特願２００４－０２５０１５
受付番号	５０４００１６３５５５
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１６年　２月　３日

＜認定情報・付加情報＞

【提出日】　平成16年 2月 2日

特願２００４－０２５０１５

出　願　人　履　歴　情　報

識別番号　［５０１１７５２８１］

１．変更年月日　２００１年　４月２７日
［変更理由］　新規登録
住　所　宮城県仙台市青葉区南吉成六丁目６番地の３
氏　名　株式会社サイバー・ソリューションズ